

GoodLinker Cloud Field View (Mobile APP) User Manual

Chapter 1 | Overview

1.1 Service Name and Applicable Versions

Name: **GoodLinker Cloud Field View** (the GoodLinker cloud platform) Interface: Mobile APP Models: GFV-S series , GFV-P series System version: APP version 4.4.6.3

1.2 Service Positioning and Functional Overview

GoodLinker Cloud Field View (hereinafter referred to as **Cloud Field View**) is a real-time factory monitoring and anomaly analysis platform built for small and medium manufacturers. The system integrates field sensor data with cloud algorithms, helping users grasp production status in real time, resolve anomalies, and improve operational efficiency.

This manual covers the "**Mobile version**," designed to give **frontline personnel** a tool for fast inspection and anomaly response. Through a mobile device, users can grasp sensor status in real time, receive anomaly push notifications, and handle issues immediately on site.

Compared with the Web version, the Mobile version focuses on **real-time data display and on-site response**, and does not include advanced functions such as AI analysis reports and sensor protocol settings.

NOTE: For advanced report analysis, the AI prediction module, and sensor protocol settings, please refer to the "Cloud Field View (Web) User Manual."

A. Primary Users

- Factory floor managers
- Equipment and production line supervisors
- Inspection personnel
- QA staff

B. Common Use Cases

- Receiving anomaly push notifications and handling them immediately on site
- Quickly switching sites or equipment groups during inspections
- Browsing real-time sensor data to grasp equipment operating status
- Reviewing daily anomaly events and statistics overview

1.3 System Highlights

- **Real-time sensor data update:** auto-refreshes every minute, or pull down to refresh manually
- **Anomaly push notifications:** instantly sends sensor alarms without logging in
- **Quick multi-site switching:** supports switching across sites and groups for centralized data management
- **Tiered permission design:** distinguishes view levels such as Owner , Administrator , and User
- **Lightweight interface:** a clean interface suited for one-handed operation and quick swiping

1.4 Use Case Summary

- **Real-time alarm notification:** quickly handle events such as downtime, temperature anomalies, and power overload
- **Daily inspection:** quickly view sensor data via tags to grasp equipment health
- **Remote monitoring:** synchronously grasp multi-equipment status across sites, supporting multi-account sharing

1.5 Interface Comparison

Item	Cloud Field View (Web)	Cloud Field View (Mobile APP)
Usage scenario	Control room, manager's desk	On-site inspection, first response to anomalies
Information scope	AI weekly report, historical data, report analysis, device settings	Real-time status, key sensors, alarm notifications
Operating role	Senior managers, IT engineers	Inspection personnel, line supervisors, QA staff
Interaction	Multi-module navigation, large-screen operation	One-handed swiping, simplified visual focus

Chapter 2 | Login & Account Activation

2.1 Download and Log In to the Mobile Service Entry

Users can download the corresponding **Mobile APP** based on their mobile platform and log in:

- **iOS APP download:** <https://apps.apple.com/tw/app/goodlinker/id1476501530>
- **Android APP download:** https://play.google.com/store/apps/details?id=com.goodlinker.mobile&pcampaignid=web_share

After launching the **Mobile APP**, you enter the login screen, which includes the following fields and buttons:

- Enter your email
- Enter password
- Forgot password
- Register
- Log in

The bottom of the screen shows version information (e.g., `version: 4.4.6.3`).

2.2 Account Registration Flow

If you do not yet have an account, register as follows:

1. Click Register
2. Fill in basic information:
 - User email
 - Password (8+ characters, alphanumeric mix required)
 - Confirm password
 - Last name
 - First name
3. Read and check to agree to the "Personal Data Statement"
4. Receive the verification code → enter the verification code → complete registration

NOTE: If you do not receive the verification code, click Resend , or contact customer service for assistance.

2.3 Account Activation and Permissions

A. First Login Prompt

After registration, on first login, if you have not joined a company organization, the system shows a prompt; please select the company to log in to.

B. Account Types and Activation

Owner

Must contact the manufacturer's service staff for back-end activation. Please provide:

- Email / username
- Company name
- Tax ID
- Address and time zone
- Contact phone
- Contact email
- The **GoodLinker IIoT Gateway** factory code (ThingName / device serial number) owned by the organization

NOTE: After activation is complete, the manufacturer will notify you by email.

User

You can join a company in the following ways:

- The Owner provides an "organization invitation code"; enter it after logging in to join
- The Owner directly adds your **email** under **Settings** → **Company Info**

NOTE: If an account has not joined a company organization, no function modules will be available.

2.4 Forgot Password

If you forget your login password, reset it as follows:

1. Click **Forgot password** on the login screen
2. The system guides you to the "Verify Email and Set New Password" page; fill in:
 - Verification code (sent by the system to the registered email)

- New password
- Confirm new password

3. If you do not receive the verification email:

- Check the spam folder
- Click the **Resend** button (the system shows a countdown and resend limit)

4. After all fields are entered, click **Done** to complete the password reset

Chapter 3 | Realtime Monitoring Dashboard

3.1 Home Screen Overview

After logging in to **Cloud Field View (Mobile)**, the system enters the **Realtime** tab by default as the home page. The screen is composed of upper and lower function areas, supporting quick browsing of sensor data and advanced operation switching.

A. Bottom Function Bar (Left to Right)

- **Overview** : enters the anomaly statistics dashboard page
- **Realtime** : shows real-time sensor data and anomaly status (default tab)
- **Menu** : goes to the account and system settings page

B. Top-Right Function Bar (Left to Right)

- **Recently viewed** : shows the list of recently browsed tags
- **Alarm list** : shows all current anomaly events and push records

C. System Language

The system automatically switches the interface based on the phone's OS language, currently supporting:

- Chinese
- English
- Vietnamese
- Thai

NOTE: After login, the default screen is the **Realtime** tab, where you can directly view the data

overview of sensor tag groups.

3.2 Realtime Page Overview

After entering the **Realtime** tab, users can quickly browse the real-time sensor data shown in each tag block (Tag). These tags are usually predefined in the **Gateway** based on production machines, monitoring sites, etc.

NOTE: Each block's data auto-updates **every minute**, or can be manually refreshed with a pull-down gesture.

A. Block Arrangement and Composition

Tag blocks are arranged as cards; each block includes:

1. **Tag name and field photo:** shown at the top of the block; if an image has been uploaded, the field photo is shown, otherwise a default icon.
2. **Status indicator (top-left of the card):**
 - **Red** : alarm
 - **Yellow** : pre-alert
 - **Gray** : disconnected (could be the Gateway or a field sensor interruption)
3. **Key sensor fields (bottom half of the card):**
 - Up to 4 selected sensor data points can be shown
 - Each field shows the sensor name, current value, and status (normal, abnormal, disconnected, etc.)

3.3 Tag Overview Screen

After tapping any tag card, you enter that tag's detailed overview screen, divided into three areas:

A. Tag Information (Top Area)

- Shows the tag name and a representative field photo
- Shows sensor status statistics (normal, abnormal, pre-alert, disconnected counts), marked by color + number

B. Key Sensors (Middle Area)

- Up to 4 selected key sensors can be shown

- Tap the **Edit** button to enter edit mode and select tracked items from all sensors

Edit mode functions:

- Selected sensors are listed at the top; drag to reorder or tap to delete
- Tap **+** in the list below to add other sensors
- Tap **Save** to apply the settings

C. All Sensors List (Bottom Area)

- Shows all sensor data under that tag
- Tap the **Sort by name** button at the top right to switch the sort method

The status color bar on the left of each sensor card:

- **Green** : normal
- **Yellow** : pre-alert
- **Red** : alarm
- **Gray** : disconnected
- If disconnected, the value field shows prompts such as "LESI disconnected" or "sensor disconnected," indicating the interruption source

NOTE: The tag overview page data auto-updates every minute, or can be manually refreshed by pulling down to get the latest data.

3.4 Sensor Card Content

After tapping any sensor card, you enter that sensor's detailed data chart page, divided into top, middle, and bottom areas:

A. Title and Settings (Top Area)

- Shows the sensor name, its tag, and equipment type
- Can set the **time zone** (default **UTC+08:00**)
- Can select a date range (default shows yesterday's data; supports today or custom date queries)

B. Chart Display Area (Middle Area)

- Automatically loads the corresponding chart based on the sensor data type (see 3.5 for chart descriptions)
- Can switch **time granularity** (e.g., **3 min** , **30 min** , **60 min**)
- Anomalous data is marked with a "red segment"; disconnected segments are shown as "blank"

C. Timeline Operation (Bottom Area)

- Drag to zoom the timeline range (default 00:00 – 24:00)
- Can focus on data for a specific period (e.g., 9 AM to 12 noon)

3.5 Sensor Data Chart Modes

The following explains the chart display for each sensor data type, including single-day and multi-day modes.

A. Lamp (Indicator-Light Status Type)

- Chart menu: green, yellow, red, blue, white, no light (selectable)
- Time granularity: 3 minutes

Single-Day Mode

- Y-axis: 24-hour timeline (00:00–24:00)
- X-axis: the segments where each light status appears (counted in seconds)
- Anomaly status: marked with red blocks
- Disconnection status: shown as blank segments

Multi-Day Mode

- Y-axis: date (e.g., 6/1–6/7)
- X-axis: total daily hours of each light status
- Anomaly count: marked in red above the chart

B. Detector (Switch Status Type)

- Chart menu: enabled status (On / Off)
- Time granularity: 3 minutes

Single-Day Mode

- Y-axis: 24-hour timeline
- X-axis: On / Off status (if On at any point within 3 minutes, recorded as On)
- Anomaly status: marked with red blocks
- Disconnection status: shown as blank segments

Multi-Day Mode

- Y-axis: date

- X-axis: daily On status percentage (e.g., 55%)
- Anomaly count: marked in red above the chart

C. Counter (Counter Type)

- Chart menu: real-time count, cumulative count (switchable)
- Time granularity: 3 minutes

Single-Day Mode

- Y-axis: 24-hour timeline
- X-axis: count
 - Real-time count : resets daily (per Gateway settings)
 - Cumulative count : the value keeps accumulating
- Anomaly status: marked with red blocks
- Disconnection status: shown as blank segments

Multi-Day Mode

- Y-axis: date
- X-axis: daily count value
- Anomaly count: marked in red above the chart

D. Timer (Timer Type)

- Chart menu: real-time timing, cumulative timing (switchable)
- Time granularity: 3 minutes

Single-Day Mode

- Y-axis: 24-hour timeline (00:00 – 24:00)
- X-axis: seconds (timing value)
 - Real-time timing : the value auto-resets at a designated cycle (per Gateway settings)
 - Cumulative timing : the value keeps accumulating
- Anomaly status: marked with red blocks
- Disconnection status: shown as blank segments

Multi-Day Mode

- Y-axis: date (e.g., 2025/06/01 – 2025/06/07)
- X-axis: total daily timing seconds

- Anomaly count: marked in red above the chart

E. Analog (Numeric Type)

- Chart menu: average, maximum, median, minimum, standard deviation (selectable)
- Time granularity: 3 min / 30 min / 60 min

Single-Day Mode

- Y-axis: 24-hour timeline
- X-axis: value change (presented per the selected statistic method)
 - Display: a line chart showing the statistic value changes within each time granularity
- Anomaly status: marked with red blocks
- Disconnection status: shown as blank segments

Multi-Day Mode

- Y-axis: date
- X-axis: the daily result of each statistic item
- Anomaly count: marked in red above the chart

NOTE: Use the "statistic method menu" to interpret data from different angles (e.g., choose "maximum" to view peaks, or "standard deviation" to observe stability).

Chapter 4 | Overview Statistics

The **Overview** page of the Mobile **Cloud Field View** provides a statistical overview of alarm events, helping users quickly grasp anomaly trends and key group distribution. Through graphical presentation, recent anomaly hotspots and frequency can be effectively identified.

4.1 Page Structure

After entering the **Overview** tab, the screen mainly comprises two areas:

A. Total Anomaly Alarm Statistics (Top Area)

- Shows the combined anomaly alarm count of all tag groups (e.g., "20 alarms total")
- Presented as icon + number for a clear data overview
- Tap this area to jump directly to the **Alarm List** to view details of each anomaly event

B. Group Alarm Statistics List (Bottom Area)

- Shows the following for each group:
 - Group name (e.g., 204-Alarm)
 - Current total alarm count (e.g., "20 total")
 - Right-side bar chart: visually shows that group's relative proportion of the total anomalies

NOTE: The system allows a sensor tag to belong to multiple groups simultaneously, or anomaly events to be shown repeatedly at different levels. Therefore, the "total anomaly count" and the "sum of each group's statistics" do not correspond one-to-one; this is normal, caused by the multi-dimensional data tracking design.

4.2 Usage Recommendations

- Recommended as a "quick anomaly navigation entry" during daily inspections
- When anomalies cluster in a specific group, you can:
 - Tap the total alarm count to jump to the Alarm list and check historical anomaly records
 - Tap any group field to further view that group's anomaly event distribution and time records

Chapter 5 | Alarm List

5.1 Function Overview

The Alarm list provides real-time anomaly event information and supports switching between "Today's Alarms" and "Yesterday's Report":

- **Today's Alarms:** shows all anomaly events of the day in real time, supporting auto and manual refresh
- **Yesterday's Report:** shows the previous day's anomaly statistics charts (see 5.3)

5.2 Today's Alarms

Each alarm is shown as a card, including the sensor name, its tag, alarm description, time of occurrence, and duration (if applicable).

NOTE: New anomaly events are added to the list in real time, or can be manually refreshed by

pulling down.

A. Sensor Types and Supported Status

Sensor type	In-progress status	Ended status	Description
Lamp	✓	✓	Shown by light value (green / red / yellow / blue / white / none)
Analog	✓	✓	Shows the high / low alert range
Detector	✗	✓	Records only status changes
Counter	✗	✓	Shows the count exceeding the threshold
Timer	✗	✓	Shows the time exceeding the threshold

B. Alarm Card Styles

In-progress status (applies to Lamp, Analog)

🔴 Current status is {ruleName} {ruleValue}
Occurred at {snsTimestamp}

Ended status (applies to all types)

🔴 Status was {ruleName} {ruleValue}
Lasted hh h mm m ss s
Occurred at {snsTimestamp}

Analog special cases (examples):

Exceeding the High/Low range:

🔴 Exceeds the safe range {ruleValueLow} ~ {ruleValueHigh} {unit}

Only High has a value:

🔴 Above the safe range {ruleValueHigh} {unit}

Only Low has a value:

🔴 Below the safe range {ruleValueLow} {unit}

NOTE: The alarm card style automatically applies the corresponding content based on the sensor type and event status.

5.3 Yesterday's Report (Alarm Summary)

Yesterday's Report provides a statistical analysis of the previous day's alarm events, supporting two view modes, switchable from the top menu:

A. Occurrence Count Mode

- A bar chart shows the distribution of yesterday's hourly alarm counts
 - **X-axis:** 0–23 hours
 - **Y-axis:** number of alarm events per hour
- Tap any period to expand the anomaly event list within that period
- The total alarm counts of each tag group are shown below to help identify concentrated anomaly areas

B. Duration Mode (applies only to Lamp , AnaLog)

- A pie chart shows the proportion of each tag's cumulative anomaly duration
 - E.g., 204-Alarm: 6 h 38 m , Total Power: 5 h 58 m
- Provides a visual basis for anomaly hotspots, useful for identifying high-risk equipment
- Tap the chart to expand the detailed anomaly event list

C. Detailed Event List (shared by both modes)

Each event card shows:

- Sensor name
- Its tag
- Anomaly description (status)
- Time of occurrence
- Duration (if applicable)

TIP: Before daily inspections, review the Yesterday's Report page first to quickly grasp trends and potential anomaly risks.

5.4 Push Notification

If push notifications are enabled in `Settings` , when the system detects an anomaly event, it instantly notifies the user via mobile push.

The push content is concisely presented in the corresponding format based on the sensor type and anomaly rule. After tapping the push message, the system automatically navigates to the `Alarm list` page to view detailed records.

A. Push Field Format

Field	Description
<code>LESI</code>	The name of the Gateway device issuing the alarm
<code>sensor</code>	The sensor alias
<code>alarm</code>	The name of the rule that triggered the alarm
<code>value</code>	The sensor value at the time of the anomaly
<code>setting</code>	The set alert value or anomaly condition
<code>thingName</code>	The Gateway 's factory code
<code>sensorType</code>	The sensor data type (e.g., <code>Analog</code> , <code>Timer</code>)
<code>sensorId</code>	The sensor ID

B. Push Content Examples (by Sensor Type)

Lamp (Indicator-Light Status Type)

 `{sensor}` light changed to `{setting}`
Detected `{sensor}` `{alarm}`; abnormal status!

Supported light values:

Setting value	Display text
green	Green light
red	Red light
yellow	Yellow light
white	White light
blue	Blue light
none	No light

Detector (Switch Status Type)

 {sensor} status changed to {value}
Detected {sensor} {alarm}; status changed to {value}!

Counter (Counter Type)

 {sensor} count anomaly
Detected {sensor} {alarm}; cumulative count reached {value}, alert value {setting}!

Timer (Timer Type)

 {sensor} time anomaly
Detected {sensor} {alarm}; cumulative time reached {value}, alert value {setting}!

If `value` or `setting` exceeds 60 seconds, the time is automatically converted to:

- `hh h mm m ss s` format
- Units of 0 are not shown (e.g., 3603 seconds → 1 h 3 s)

Analog (Numeric Type)

 {sensor} value exceeds the safe range
Detected {sensor} {alarm}; reached {value}, exceeding the safe range {setting}!

C. Notes

- Push notifications operate based on account login status: if the same account is logged in on multiple devices, only the **last logged-in device** receives notifications.
- Push is only an auxiliary reminder; even if no notification is received, the anomaly event is still fully recorded in the system.

TIP: Each user should use an independent account to ensure push notifications are delivered accurately and to avoid missing alarms due to shared accounts.

Chapter 6 | Menu & Settings

The **Menu** page in the app provides personal and company-related function settings, helping users with account management, password changes, organization queries, and equipment monitoring.

This chapter explains the content and use of each function area in the **Menu**.

6.1 Function Categories

The **Menu** page is divided by function into two areas:

A. Personal Function Area

- **Alarm Notification** : set whether to receive anomaly pushes
- **User Profile** : view and update personal basic information
- **Change Password** : modify the login password
- **Biometric Login** : set up face or fingerprint login (depending on device support)

B. Company Function Area

- **Company Info** : view the affiliated company's basic information and company code
- **Member List** : browse the list of all users in the organization; only some roles have management permission
- **Device Management** : view the status and identifiers of connected LESI devices in the company

6.2 Alarm Notification

- Provides a **switch** to set whether to receive anomaly alarm pushes on the mobile device
- After turning off push, the system still records anomaly events but does not actively send notifications
- If the same account is logged in on multiple devices, only the "last logged-in" device receives pushes
- It is recommended that each user create an independent account to ensure pushes are delivered accurately

6.3 User Profile

- Shows the account's email, name, and configured time zone
- The `Delete Account` operation is available:
 - After tapping, you are redirected to an online survey form
 - After filling in the form, the manufacturer's customer service handles the deletion request
 - You are notified by email after processing is complete

6.4 Change Password

- Provides the function to modify the login password
- Requires entering the following three items:
 - `Current password`
 - `New password`
 - `Confirm new password` (re-enter the new password to verify)
- Password format requirement: at least 8 characters, with an alphanumeric mix

6.5 Biometrics

- Enables the mobile device's built-in biometric function (e.g., Face ID or fingerprint)
- Once enabled, the login screen supports quick login

6.6 Company Info

- Shows the basic information of the company the logged-in account belongs to:
 - `Company name`
 - `Subscription plan` (e.g., Free / Basic / Premium)
 - `Available license seats` (current usage and the limit)

6.7 Member List

- Lists all member accounts in the current company organization
- Identifies account types:
 - `Owner`
 - `User`
- Shows the currently used license count and limit

6.8 Device Management (Device Info & Disconnection Log)

The **Device Management** page lets users view the communication status and disconnection records of each Gateway and its connected field equipment (such as PLCs and sensors), helping to grasp connection stability and troubleshoot anomalies. Common scenarios:

- Confirming whether the anomaly source is "Gateway offline" or "equipment communication interruption"
- Tracking the time of communication interruptions and whether they auto-recovered
- Analyzing interruption frequency to judge whether it relates to network or equipment faults

NOTE: This page only provides status display and record viewing; it cannot perform remote control or device settings.

A. Gateway Disconnection Records

- Shows each Gateway's connection and disconnection time records
- The information shown is the Gateway body's connection status, not directly related to sensor data transmission
- The Gateway has a disconnection buffering mechanism, storing about 120 hours of data, and automatically uploads after reconnecting

Fields include:

Field	Description
Device name	The Gateway display name
Device serial number	The factory code (ThingName)
Status	Online / disconnected (shown by color icon)
Time of occurrence	The time of the connection status change (with hour, minute, second)

B. Field Equipment Disconnection Records (PLC / Sensor)

- Shows the communication interruptions of field equipment connected to each Gateway
- Once equipment disconnects, the system cannot capture that channel's real-time data

Fields include:

Field	Description
Protocol	The protocol type used by the equipment (e.g., TCP)
Equipment alias	The equipment IP or identifier
Disconnection time	The last communication interruption time (precise to the second)

NOTE: If equipment disconnects frequently, check the field wiring, IP configuration, or network communication parameters.

6.9 Switch Company

- When an account has permissions for multiple companies, this function switches the company organization to log in to
- After selecting the target company, you can log in to that company's data space

6.10 Logout

- Provides a secure logout function
- After tapping, a confirmation prompt appears: "Confirm logout?"

Chapter 7 | Related Documents

This chapter lists other operation guides related to this manual, recommended for reference to fully understand the overall system architecture and operation logic.

- **GoodLinker IIoT Gateway User Manual**
 - For detailed setup and functional description of the Gateway hardware (Device Configuration Manual)
- **GoodLinker Cloud Field View (Web) User Manual**
 - For the back-end cloud management platform, including dashboard, alarm, and reporting operations (Cloud Dashboard Web Manual)
- **GoodLinker Cloud Field View (Mobile APP) User Manual**
 - For phone and tablet operation, supporting real-time queries and anomaly notifications (Mobile App Operation Guide)

Chapter 8 | History of Specification

This chapter lists the version evolution of this service's user manual and related functions, helping users understand the product update history.

Version	Release date	Author / Reviewer	Update notes
v1.0.0	2019/11/20	Bruce King	Initial release
v2.0.0	2025/06/03	Bruce King	Full revision: new user manual, chapter restructuring
v3.0.0	2026/06/01	Bruce King	Content update and revision

Chapter 9 | ISV Information

This service is developed by GoodLinker Co., LTD. If you encounter any issues during installation, setup, or use, please contact us through the following:

Item	Information
Company	GoodLinker Co., LTD.
Website	https://goodlinker.io/
Product page	https://www.goodlinker.io/product/bcs-m100
Email	info@goodlinker.io
Phone	+886-2-2599-7987
Address	GoodLinker Co., Ltd. No. 40, Sec. 3, Zhongshan N. Rd., Zhongshan Dist., Taipei City 104327, Taiwan (R.O.C.)

TIP: For more detailed operation instructions, return to the corresponding chapter of this manual, or contact our technical support team for assistance.